REMARKS/DISCUSSION OF ISSUES

By this Amendment, Applicants: amend claims 1, 4, 7-9, 12, 15-16 and 21; cancels claims 6 and 14; and adds new claims 23-24. Claims 1 and 9 are amended to restore these claims to their original scope, and to make minor formal corrections. Claims 7, 8, 15 and 16 are amended to make minor formal corrections. Claim 21 is amended to broaden its scope to be commensurate with the disclosure. New claims 23 and 24 are added to include dependent elements which have been removed from claims 1 and 9 when restoring these claims to their original scope.

Accordingly, claims 1-5, 7-13, and 15-24 are pending in the application.

The Examiner is respectfully requested to acknowledge the claim for priority and receipt of certified copies of all the priority documents.

35 U.S.C. § 103

The Office Action rejects claims 1-22 under 35 U.S.C. § 103 over Aucsmith U.S. Patent 5,712,800 ("Aucsmith") in view of Marino et al. U.S. Patent 6,026,165 ("Marino") and further in view of Traw U.S. Patent 6,542,610 9 ("Traw").

Applicants respectfully submit that all of the pending claims are clearly patentable over the prior art for at least the following reasons.

Claim 1

At the outset, in the system of claim 1, each of the receivers is associated with a corresponding set of a plurality of device keys.

Applicants see no mention in the Office Action of the feature that each receiver is associated with such a plurality of key devices.

Therefore, Applicants respectfully submit that claim 1 is patentable over the cited prior art.

Also among other things, in the system of claim 1 the transmitter includes means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key.

None of the cited references disclose such a feature, and therefore no possible combination of the cited references could ever produce a system including such a feature.

Aucsmith discloses a system which distributes a master key (K) from a transmitter (10) to a plurality of receivers (20-38) by encrypting a single unique value, X, to obtain X', and then broadcasting the value X' to all of the receivers. Each individual receiver uses its private key (k(i)) and its prime number (p(i)) to decode therefrom the master key, K (see col. 10, line 14 through col. 11, line 25). So, clearly, Aucsmith does not include any means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key. Indeed, such an operation would be directly contrary to Aucsmith's teachings and fundamental purpose.

Therefore, Aucsmith does not disclose a transmitter including means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key.

Meanwhile, Marino discloses a security system with a plurality of transmitting devices (2), each transmitting to only **one** receiving device (6) which is wired to a control unit (8) for the security system. Marino teaches that the transmissions of some of the transmitting devices (2) may be encrypted by an encoder module (7). Marino has plural device IDs – one for each transmitting device (2). However, Marino does not disclose any plurality of device keys for a plurality of receivers. More specifically, Marino does not disclose any key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, or any transmitting device that would transmit any such key block.

Even more specifically, Marino does not disclose any key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, or any transmitting device that would transmit any such key block in FIG. 3 item 30, FIG. 4 item (B), col. 1 lines 63-66, and col. 9, lines 49-58. For example: FIG. 3 item 30 is a (singular) transmitter's device ID field in a received transmission; FIG. 4 item (B) shows a encrypted transmission message format that does **not** include any plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key; col. 1, lines 63-65 merely states that many different encryption and decryption algorithms exist; and col. 9 lines 49-58 merely states that more than one transmitting device can be learned, with each such transmitting device having its own random encryption key associated with its device ID.

Therefore, Marino does not disclose a transmitter including means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key.

Finally, Traw discloses a method of protecting digital content from unauthorized copying and sharing when being transferred over an insecure link. In this method, a device having the protected content (content source) and another device to which it is desired to transfer the protected content (content sink) engage in a challenge and verification process over a control channel using a shared secret key.

Traw does not disclose a transmitter including means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key.

So, neither Aucsmith, Marino, nor Traw disclose a transmitter including means

for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key. Therefore no possible combination of Aucsmith, Marino, and Traw could ever produce the system of claim 1 including such a feature.

Furthermore, Applicants also traverse the proposed combination of references as totally lacking any motivation or suggestion whatsoever in the prior art.

As noted above, Aucsmith discloses a system which distributes a master key (K) from a transmitter (10) to a plurality of receivers (20-38) by encrypting a single unique value, X, to obtain X', and then broadcasting the value X' to all of the receivers. Meanwhile, and in stark contrast, Marino discloses a system with a plurality of transmitting devices (2) all configured to transmit their individual keys (there is no master key) to a single receiver 6.

The Office Action states that it would have been obvious to combine the teachings of Aucsmith and Marino "in order to have a secure system whereby only authorized and selected receiver can decrypt the messages in as (sic) taught by Marino," citing col. 7, lines 57-65.

However, col. 7, lines 57-65 of Marino doesn't say anything at all about "a secure system whereby only authorized and selected receiver can decrypt the messages." Nor, more specifically, does the cited text teach that a transmitter includes means for transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least some of the entries containing a representation of the authorization key encrypted with the associated device key, "in order to have a secure system whereby only authorized and selected receiver can decrypt the messages." Nor is this taught anywhere else in Marino.

Therefore, Applicants respectfully submit that the proposed combination of Aucsmith and Marino with respect to claim 1 is improper, lacking any motivation or suggestion at all in the prior art.

Furthermore, Traw is only cited for its supposed disclosure of receivers

sharing a key. However, since shared keys are no longer recited in claim 1, Traw would appear to be irrelevant to claim 1.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 1 is patentable over the cited prior art.

Claims 2-5, 7-8 and 19-20

Claims 2-5, 7-8 and 19-20 depend from claim 1 and are deemed patentable for at least the reasons set forth above with respect to claim 1, and for the following additional reasons.

Claims 3-5

Among other things, in the system of claim 3 the transmitter is operative to disable decryption of the data in a receiver by changing the authorization key and transmitting a key block wherein entries associated with device keys which are associated with a receiver to be revoked contain values other than the representation of the authorization key encrypted with the associated device key.

The Office Action merely states that Aucsmith discloses the disabling of decryptors.

But of course that is not what is recited in claim 3. The Office Action fails to mention the feature wherein entries associated with device keys which are associated with a receiver to be revoked contain values other than the representation of the authorization key encrypted with the associated device key.

Similarly, among other things, in the system of claim 4 the transmitter is operative to re-enable decryption of the data in a disabled receiver by changing the authorization key and transmitting a key block wherein at least one of the entries associated with device keys which are associated with a receiver to be re-enabled contains the representation of the authorization key encrypted with the associated device key.

The Office Action merely states that Aucsmith discloses the re-enabling of reception by previously disabled receivers "by changing key (sic) and associated device keys."

But of course that is not what is recited in claim 4. The Office Action fails to

mention the feature of transmitting a key block wherein at least one of the entries associated with device keys which are associated with a receiver to be re-enabled contains the representation of the authorization key encrypted with the associated device key.

Meanwhile, among other things, in the system of claim 5, the transmitter is operative to renew a set of device keys of a specific receiver by transmitting to the receiver a new set of device keys encrypted under control of a fixed device key that is unique for the receiver, and wherein the receiver is operative to receive a set of encrypted device keys, and the receiver includes a third decryptor for decrypting the set of encrypted device keys under control of a fixed device key that is unique for the receiver.

The Office Action merely states that Aucsmith discloses the disabling of decryptors, disabling of reception, & replacement (renewing) and revocation of keys.

But, again, of course that is not what is recited in claim 5. The Office Action fails to mention the feature of transmitting to the receiver a new set of device keys encrypted under control of a fixed device key that is unique for the receiver, and wherein the receiver is operative to receive a set of encrypted device keys, and the receiver includes a third decryptor for decrypting the set of encrypted device keys under control of a fixed device key that is unique for the receiver.

Respectfully, Applicants have paid the appropriate claim fees for this application. Applicants are entitled to a full and complete examination of each and every pending claim, including all features recited therein. If the Examiner cannot cite prior art taken alone or in combination which would have produced the systems of claims 3-5, including ALL of their recited features, then Applicants respectfully submit that they are entitled to an allowance of these claims as a matter of law. Accordingly, the Examiner is respectfully requested to cite something in the prior art disclosing systems including all of the features recited in claims 3-5, or else allow Applicants' claims.

Claim 9

At the outset, in the system of claim 9, each of the receivers is associated with

a corresponding set of a plurality of device keys.

Applicants see no mention in the Office Action of the feature that each receiver is associated with such a plurality of key devices.

Therefore, Applicants respectfully submit that claim 9 is patentable over the cited prior art.

Also among other things, in the system of claim 9 the transmitter is configured to transmit to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least one of the entries containing a representation of the authorization key encrypted with the associated device key.

As explained above with respect to claim 1, no combination of the cited references would produce a system including such a feature.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 9 is patentable over the cited prior art.

Claims 10-13 and 15-18

Claims 10-13 and 15-18 depend from claim 9 and are deemed patentable for at least the reasons set forth above with respect to claim 9, and for the following additional reasons.

Claims 11-13

Claims 11-13 include features that, respectively, are similar to features of claim 3-5 as discussed above.

As explained above with respect to claims 3-5, the Office Action fails to mention various features of claims 11-13.

Respectfully, Applicants have paid the appropriate claim fees for this application. Applicants are entitled to a full and complete examination of each and every pending claim, including all features recited therein. If the Examiner cannot cite prior art taken alone or in combination which would have produced the systems of claims 11-13, including ALL of their recited features, then Applicants respectfully submit that they are entitled to an allowance of these claims as a matter of law. Accordingly, the Examiner is respectfully requested

to cite something in the prior art disclosing systems including all of the features recited in claims 11-13, or else allow Applicants' claims.

Claim 21

In the method of claim 21, each of the receivers is associated with a corresponding set of a plurality of device keys.

Applicants see no mention in the Office Action of the feature that each receiver is associated with such a plurality of key devices.

Therefore, Applicants respectfully submit that claim 21 is patentable over the cited prior art.

Also among other things, the method of claim 21 includes transmitting to all receivers a same key block with a plurality of entries, where each entry is associated with a respective different device key, at least one of the entries containing a representation of the authorization key encrypted with the associated device key.

As explained above with respect to claim 1, no combination of the cited references would produce a method including such a feature.

Accordingly, for at least these reasons, Applicants respectfully submit that claim 9 is patentable over the cited prior art.

Claim 22

Claim 22 depends from claim 21 and is deemed patentable for at least the reasons set forth above with respect to claim 21.

NEW CLAIMS 23-24

New claims 23-24 depend respectively from claims 1 and 9 and are deemed patentable for at least the reasons set forth above with respect to claims 1 and 9, and for the following additional reasons.

In the systems of claims 23 and 24, at least some device keys are shared between at least two of the receivers.

Applicants respectfully submit that no combination of the cited references would produce a system including such a feature. In particular, Applicants respectfully submit that there is no motivation to modify Aucsmith's system to include such a feature "in order to make authentication possible." The Office Action fails to

explain why anyone would ever need any authentication in Aucsmith, and even if one did, why that would have motivated anyone to modify Aucsmith's system such that at least some device keys are shared between at least two of the receivers. Indeed, such shared keys appear to be directly contrary to the teachings of Aucsmith, as that would destroy the ability for Aucsmith to enable and disable each receiver individually.

Accordingly, for at least these additional reasons, Applicants respectfully submit that claims 23 and 24 are patentable over the cited prior art.

CONCLUSION

In view of the foregoing explanations, Applicants respectfully request that the Examiner reconsider and reexamine the present application, allow claims 1-5, 7-13, and 15-24 and pass the application to issue. In the event that there are any outstanding matters remaining in the present application, the Examiner is invited to contact Kenneth D. Springer (Reg. No. 39,843) at (571) 283.0720 to discuss these matters.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment (except for the issue fee) to Deposit Account No. 50-0238 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17, particularly extension of time fees.

Respectfully submitted,

VOLENTINE FRANCOS & WHITT, P.L.L.C.

Date: 6 June 2006

By: _____
Kenneth D. Springer
Registration No. 39,843

VOLENTINE FRANCOS & WHITT, P.L.L.C.
11951 Freedom Drive, Suite 1260
Reston, Virginia 20190
Telephone No.: (571) 283.0724
Facsimile No.: (571) 283.0740